编号：JR-001[2016]

国家信息安全漏洞库
兼容性服务白皮书

中国信息安全测评中心

目录

第1章　引言

国家信息安全漏洞库（“China National Vulnerability Database of Information Security”，简称“CNNVD”），是中国信息安全测评中心为切实履行漏洞分析和风险评估的职能，负责建设运维的国家信息安全漏洞库，为我国信息安全保障提供基础服务。通过自主挖掘、社会提交、协作共享、网络搜集以及技术检测等方式，经过多年的收录工作，CNNVD 已收录信息技术产品漏洞信息 8 万余条，信息系统相关漏洞信息 6 万余条，漏洞信息覆盖国内外主流的应用软件、操作系统和网络设备等，涉及国内外各大厂商上千家，涵盖政府、金融、交通、工控、卫生医疗等多个行业。随着 CNNVD 漏洞库漏洞数量不断扩大、影响力逐步提升，目前成为收录漏洞数目最多、漏洞属性最全、内容质量最高的国家级信息安全漏洞库。

CNNVD 作为国家信息安全漏洞库，通过多年建设经验积累，对国内信息安全技术国家标准，及国际通用标准进行了分析与研究，并以国家标准为基础，参考国际通用标准，完成了国内外主流漏洞库的漏洞信息资源规范化的整合，建立了规范统一漏洞数据标准，包括：《CNNVD 漏洞编码规范》、《CNNVD 漏洞命名规范》、《CNNVD 漏洞分级规范》、《CNNVD 漏洞内容描述规范》、《CNNVD 漏洞分类描述规范》、《CNNVD 漏洞影响实体描述规范》。

CNNVD 漏洞库对所收录的漏洞信息给予统一的编码标识（即：CNNVD-ID 标识），建立了与国内外主流漏洞库的映射关系，同时对漏洞详细属性特征进行统一的、详细的、标准化的描述（如：漏洞命名、内容描述、分类、分级等），基本涵盖了国内外主流软硬件产品和信息系统。

以丰富标准的漏洞数据为依托，规范详实的漏洞描述为基础，国家信息安全漏洞库（CNNVD）对国内外信息安全厂商及用户推出兼容性服务，为漏洞挖掘、应用、验证与规避等技术研究提供基础支持，为开发更安全的信息产品或软件系统提供理论和技术支撑，进一步满足国家重要信息系统安全保障的需求。

第2章　CNNVD 兼容性服务业务介绍

2.1 服务定义

CNNVD 兼容性是指通过使用 CNNVD 标识，在各类安全工具、漏洞数据存储库及信息安全服务之间，以及与其他漏洞披露平台之间，实现漏洞信息交叉关联的方式。**CNNVD 兼容性服务**是 CNNVD 面向国内外信息安全从业单位，对其产品/服务等涉及的漏洞信息进行规范性评估与认证的服务。通过 CNNVD 兼容性服务的信息安全产品/服务，可实现其漏洞信息拥有统一的规范性命名与标准化描述，从而提高和加强国内信息安全行业漏洞信息资源的共享与服务能力。

通过 CNNVD 兼容性服务的产品/服务，应满足 CNNVD 兼容性的要求：第一，检索要求，通过 CNNVD 标识可检索到对应的漏洞信息；第二，输出要求，在输出的漏洞信息中应包含 CNNVD 标识；第三，更新要求，存储数据库需定期更新 CNNVD 漏洞数据，并与 CNNVD 更新速度保持基本一致；第四，标准文档要求，产品/服务标准说明文档中需包含 CNNVD 兼容性的说明。

2.2 服务特点

唯一性：每个漏洞拥有唯一的编码标识；

及时性：CNNVD 漏洞库有专业的团队与系统工具，对各大主流漏洞库进行信息进行更新，确保数据收录的及时性；

兼容性：CNNVD 漏洞库数据源涵盖了国内外各大主流漏洞库，如 CVE、NVD、Bugtrag、ZDI、绿盟科技、启明星辰等，同时对 Microsoft、Cisco、Oracle 等重要厂商安全公告披露的漏洞信息进行了收录，实现 CNNVD 与国内外漏洞数据源的有效兼容；

规范性：在参考国内信息安全技术国家标准、国际通用标准的基础上，CNNVD 制定了统一的漏洞标准规范。

易识别：统一的命名标识与规范化的描述，能更好的让用户识别安全隐患，提高安全防护。

2.3 服务作用

- **安全厂商使用 CNNVD 兼容性服务的优势**

1. 使用 CNNVD 兼容性服务的安全厂商，可让自身的安全产品/服务兼容国际标准与国家标准规范，可提供更好的安全服务，提升厂商竞争力；
2. 使用 CNNVD 兼容性服务的安全厂商，可实现与其他漏洞数据库（如 CVE）的相互映射，提升安全服务能力；
3. 使用 CNNVD 兼容性服务的安全厂商，可与 CNNVD 漏洞库进行数据同步，能第一时间获得最新漏洞与修复补丁信息，减少安全厂商在自身产品/服务基准库的资源投入，更加专注于提升自身产品/服务的防护能力；
4. 使用 CNNVD 兼容性服务的安全厂商，可基于 CNNVD 漏洞库打造、拓展更精细的创新性安全产品/服务；
5. 使用 CNNVD 兼容性服务的安全厂商，对于同用户或系统平台，可实现多类安全产品/服务相互映射，形成整体安全态势信息，便于提出安全解决方案；
6. 使用 CNNVD 兼容性服务的安全厂商，可获得 CNNVD 兼容性服务资质证书及服务标识 LOGO 的授权，提升产品/服务的用户认可度。

- **企业用户使用符合 CNNVD 兼容性要求的产品/服务的好处**

1. 对企业用户而言，使用符合 CNNVD 兼容性要求的产品/服务，可实现多个安全厂商的多类安全产品基于 CNNVD 标识相互检索、相互配合，协同解决企业安全风险和安全隐患。
2. 对企业用户而言，使用符合 CNNVD 兼容性要求的安全产品/服务，拥有统一的、符合国标的漏洞信息、补丁信息等的标准描述，可根据 CNNVD 标识，确定所采用的产品是否及时更新和升级了相关补丁。
3. 对企业用户而言，使用符合 CNNVD 兼容性要求的产品/服务，可以根据公开的漏洞预警或漏洞公告所涉及的漏洞标识，确定所采用的产品/服务是否覆盖相关漏洞。

第3章　CNNVD 兼容性服务内容

3.1 服务对象

CNNVD 兼容性服务主要面向国内外信息安全从业单位，对其提供安全服务（如入侵检测、终端安全、网站监测、漏洞扫描等）的工具（软/硬）、系统、平台或其他安全产品所涉及的漏洞信息提供规范化服务。

3.2 申请流程

CNNVD 兼容性服务申请流程分为五个阶段：

第一阶段，申请单位提交用户与产品的申请材料和资质证明；**第二阶段**，申请单位等待 CNNVD 进行资料审核，收到审核通过的通知后，提交兼容性测试结果，CNNVD 与通过评审的单位签订兼容性服务协议；**第三阶段**，申请单位落实兼容性要求，CNNVD 对其实施情况进行现场确认并进行专家评审；**第四阶段，**CNNVD 对完成兼容性服务的产品颁发资质证书并公示。**第五阶段，**协议有效期内，CNNVD 对通过兼容性服务的产品进行实施监督。

其过程共分为八个步骤：1、**用户提交申请**；2、**资料审核**；3、**兼容性测试**；4、**兼容性综合评估**；5、**签订兼容性服务协议**；6、**兼容性实施确认与评审**；7、**颁发证书并公示；8 兼容性实施监督**。CNNVD 兼容性服务申请流程如图 1 所示：

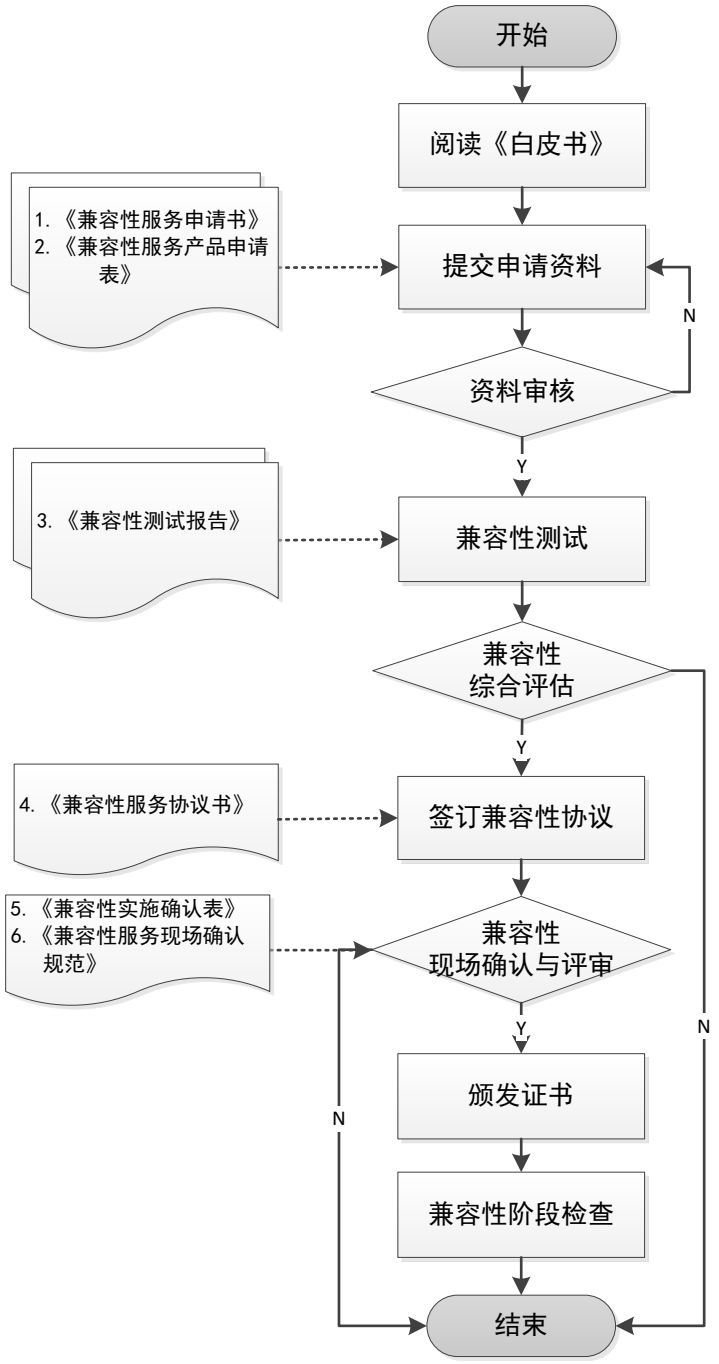

图 1　CNNVD 兼容性服务申请流程

1. 用户提交申请

申请 CNNVD 兼容性服务的用户，需发送邮件至 cnnvd@itsec.gov.cn 获取《CNNVD 兼容性申请书》和《CNNVD 兼容性产品申请表》，按照要求填写好后，须将申请表及其他相关资料的电子版发送至 CNNVD 邮箱予以确认，并于 5 个工作日将纸质版资料（加盖公章）邮寄至中国信息安全测评中心。

注：已通过兼容性服务的单位，申请其他产品时仅提交《CNNVD 兼容性产

品申请表》即可。《申请书》如有内容变更，则须重新提交。

2. 材料审核

CNNVD 将于 5 个工作日内对申请单位所提交的相关资料进行审核，审核内容包括：对申请单位的资本资料和相关资质进行审核；对申请产品/系统的基本资料和相关资质进行审核。审核结果会以邮件方式告知。

3. 兼容性测试

通过资料审核后，CNNVD 会向申请单位提供《CNNVD 兼容性服务测试报告》模板及 XML 格式的样本数据，申请单位要在 5 个工作日内完成自测并将测试资料（纸质版和电子版）反馈给 CNNVD。

4. 兼容性综合评估

CNNVD 将按照“服务要求”评估标准，对申请产品/服务进行兼容性综合评估，评估结果以邮件方式告知。

5. 签订兼容性服务协议

根据综合评估结果，对于申请通过的产品/服务，中国信息安全测评中心与申请单位签订《CNNVD 兼容性服务协议书》。

6. 兼容性实施确认与评审

兼容性服务协议书签订后，申请单位需在 20 个工作日内完成兼容性落实工作，如未能按时在实施期内完成，须提前向 CNNVD 提出延期申请，最终实施期不得超过 40 个工作日，并将完成情况邮件告知。然后，由 CNNVD 发送《CNNVD 兼容性服务实施确认表》与《兼容性服务现场确认规范》，申请单位将该表填好后予以反馈，由 CNNVD 对其实施情况进行现场确认与专家评审，确保兼容性服务的贯彻实施。

7. 颁发证书并公示

兼容性实施现场确认与评审通过后，CNNVD 对实施完成的产品将颁发 CNNVD 兼容性服务资质证书，并在 CNNVD 官方网站进行发布。

8. 兼容性实施监督

CNNVD 颁发证书后，在协议有效期内将对已通过兼容性服务的产品进行实施监督，监督机制具体见第 4 章。

3.3 服务要求

对于通过 CNNVD 兼容性服务的产品/服务及所属厂商，需满足 CNNVD 兼容性服务的**基本要求**与**功能要求**。

3.3.1 基本要求

凡通过 CNNVD 兼容性服务的产品/服务及所属厂商，需遵守以下基本要求：

1. 厂商必须遵守相关法律法规，其产品/服务不得侵犯任何第三方的专利权、著作权、商标权、名誉权或其他任何合法权益；
2. 厂商所提交的各类材料（资质证明材料、产品技术材料等）须真实有效；通过 CNNVD 兼容性服务的产品/服务与厂商所属关系发生变化时，须提前告知 CNNVD，并提供变更后的厂商资料；
3. 通过 CNNVD 兼容性服务的同款产品/服务版本升级须告知 CNNVD，进行备案；若版本迭代须重新申请 CNNVD 兼容性服务；
4. 通过 CNNVD 兼容性服务的厂商须提供接口人，以协调 CNNVD 兼容性服务相关工作；
5. 对于通过 CNNVD 兼容性服务的产品/服务，CNNVD 授权使用兼容性服务的 LOGO，产品/服务须将 LOGO 进行贴注，具体要求如下：
   （1） 软件系统，须在系统界面添加 CNNVD 兼容性服务标识 LOGO。
   （2） 硬件设备，须在设备外壳及外包装盒添加 CNNVD 兼容性服务标识 LOGO，同时在设备系统内添加 CNNVD 兼容性服务标识 LOGO。

3.3.2 功能要求

通过 CNNVD 兼容性服务的产品/服务必须满足以下功能要求：

1. CNNVD 标识检索要求

通过申请的产品/服务须保证使用 CNNVD 标识检索到相关漏洞信息。

2. CNNVD 标识输出要求

通过申请的产品/服务，其输出的相关信息中，必须包含 CNNVD 标识；

3. CNNVD 漏洞更新要求

对于配有存储库的产品/服务，其漏洞信息必须能与 CNNVD 标识进行一一映射匹配，且更新速度与 CNNVD 漏洞信息的更新速度基本一致。

4. 产品/服务的标准说明文档要求

（1）相关的标准说明文档（或帮助文档）须包括 CNNVD 和 CNNVD 兼容性服务的简要描述，可参考《CNNVD 兼容性服务白皮书》；

（2）相关的标准说明文档（或帮助文档）须说明用户如何通过 CNNVD 标识检索漏洞信息，以及通过漏洞信息查询其 CNNVD 标识；

（3）相关的标准说明文档（或帮助文档）如包含索引，必须在相关说明中标出引用。

3.4 证书续期

兼容性服务资质有效期为三年。相关单位应在有效期结束之前向 CNNVD 提交续期申请和变更声明。未提交申请或未成功办理证书续期的单位将取消兼容性服务合作，CNNVD 会对取消资质的单位进行声明和公示。

3.5 数据同步

CNNVD 漏洞库采用国际通用的“XML”标准格式对漏洞信息资源共享，用户在使用前需先了解 www.w3.org 定义的 XML 标准和相关的技术，获取“XML”格式的漏洞信息资源需登录 CNNVD 官方网站（http://www.cnnvd.gov.cn）下载“XML 文件”。

漏洞信息资源以年、月、日为时间单位提供下载使用，对应更新的频率为每月更新（月初第一个工作日）、每日更新（每日 17 点）、每日更新（每日 17 点），如了解更多信息，请登录 CNNVD 官方网站“XML 数据源文件”下载页面。

3.6 服务费用

CNNVD 兼容性服务暂不收取费用。

第4章　兼容性服务监督机制

CNNVD 兼容性服务监督机制，是对已通过并在有效期内的兼容性服务安全产品/服务进行监督的机制，其主要目的是审核兼容性服务的落实与执行情况。在监督期间，若该产品/服务未满足兼容性服务的要求，则会被警告或撤销资格。

4.1 监督要求

1、在兼容性服务有效期间内，均为 CNNVD 监督时间范围；

2、通过兼容性服务的产品/服务及所属厂商，均为 CNNVD 监督对象；

3、在兼容性服务的有效期内，厂商是否落实并贯彻执行兼容性服务基本要求。如未落实并贯彻执行，则进入警告阶段；

4、在兼容性服务的有效期内，厂商是否落实并贯彻执行兼容性服务的功能要求。如未落实并贯彻执行，则进入警告阶段；

5、在兼容性服务的有效期内，产品/服务是否涉侵、违法及损害 CNNVD 利益。如出现，则进入警告阶段，当情节严重时则直接进入撤销阶段。

6、在兼容性服务的有效期内，厂商是否存在损害 CNNVD 利益的言论、行为。如存在，则进入警告阶段，当情节严重时则直接进入撤销阶段。

7、在兼容性服务的有效期内，产品/服务所属厂商关系发生变更，则需告知 CNNVD，并及时更新厂商资料；如不告知 CNNVD，则视为申请材料不符合要求，进入警告阶段；

4.2 监督流程

监督机制包括两个阶段：警告阶段和撤销阶段，详情如下：

4.2.1 警告阶段

（1）当 CNNVD 监督期间发现问题时，会邮件告知，并要求在 5 个工作日内响应（回复邮件或电话）；如 5 个工作日内部不做出响应，则进入撤销阶段。

（2）当厂商对监督问题进行响应后，需在 10 个工作日内对问题进行处理并解决，如 10 个工作日内无法完成，可向 CNNVD 申请延长处理时间，经同意后可在规定时间内解决问题；若厂商在规定时间内未解决问题，且未向 CNNVD 申请延期，则进入撤销阶段。

（3）厂商解决问题后，需告知 CNNVD 并提交证明材料，材料可自行编写；如已解决问题但未告知 CNNVD，则视为未解决问题，直接进入撤销阶段。

4.2.2 撤销阶段

（1）当进入撤销阶段时，CNNVD 会邮件告知；

（2）进入撤销阶段的厂商及所属产品/服务，可重新按照 CNNVD 兼容性服务的申请流程再次申请，但 CNNVD 有权根据撤销原因责令其提供申请要求以外的必要材料进行审核。

（3）对于侵权、违法或损害 CNNVD 利益的厂商，必须整改满足要求后，方可重新申请 CNVND 兼容性服务；对于情节严重的，CNNVD 有权永久取消申请资格。

以上为 CNNVD 兼容性服务白皮书全部内容，本书最终解释权归中国信息安全测评中心所有。